

valid period is determined when the source IP address of the external apparatus is first stored.

In the step S105, it is judged whether or not the source IP address is within the valid period.

5 Incidentally, time lapse from the time of storing the source IP address needs to be recognized in order to judge whether or not it is within the valid period, which is made possible when what is known as a calendar function or clock function is  
10 executed through generally known software processing in the central controlling section 6.

【0026】 Then, when the source IP address is judged in the step S105 to be within the valid period (YES), the response to the external apparatus giving the  
15 access is determined to be allowable and the procedure proceeds to the processing of the step S110 (refer to the step S106 in FIG. 4).

Meanwhile, when it is judged in the step S104 that the source IP address is nonidentical with the  
20 stored source IP address, or is not within the valid period, in other words, the valid period is expired, the response to the external apparatus is determined to be unallowable (refer to the step S108 in FIG. 4) and the source IP address of the  
25 external apparatus which is judged to be

nonidentical with the stored source IP address or  
not to be within the valid period in the judgment  
in the step S104 or the step S105 is registered in  
the unauthorized access IP list (refer to the step  
5 S109a in FIG. 4). In short, when an access to the  
intelligent interconnecting device 1 from outside  
occurs and a source IP address of the external  
apparatus giving the access is judged to be  
nonidentical with the stored source IP address in  
10 the step S104, the source IP address which is judged  
to be nonidentical is stored in subsequence in the  
unauthorized access IP list which is provided in  
a predetermined area of the storage section 9 to  
register therein the source IP address which is  
15 judged to be nonidentical with the stored source  
IP address.

【0027】 In order to notify the managing computer  
4 of the source IP address which is judged to be  
nonidentical with the stored source IP address,  
20 this source IP address is then transmitted as a  
predetermined packet to the managing computer 4 via  
the LAN trunk line interfacing section 7 (refer to  
the step S109b in FIG. 4). After the processing  
of the step 109b, the procedure returns to the main  
25 routine processing and the processing for the case

in which the response to the external apparatus is determined to be unallowable is performed according to the provided TCP/IP protocol.

Incidentally, the source IP address which is judged to be nonidentical with the stored source IP address is stored (refer to the step S109a in FIG. 4) and notified to the managing computer 4 (refer to the step S109b in FIG. 4) in the above second example, but only either one of the storage and the notification may be carried out.

【0028】 Furthermore, the explanations of both the first and second examples are made on the premise that only one source IP address is stored in the intelligent interconnecting device 1 for the external apparatus whose access is permitted but it is not restrictive that only one source IP address is set and a plurality of them may of course be set.

When the intelligent interconnecting device 1 is structured to be operable under an SNMP (Simple Network Management Protocol) which is a network control protocol in a TCP/IP network, that is, when the intelligent interconnecting device 1 is provided with an SNMP agent and, for example, the managing computer 4 and other computers are also